TICOM/I-211

TOP SECRET.

PRELIMINARY INTERROGATION OF DR. HANS PETER LUZIUS OF OKH/In. 7

Attached is a report on the preliminary interrogation of Dr. Hans Peter LUZIUS, former member of the American Section of OKH/In. 7, carried out by Mr. K. L. Perrin of G.C.H.Q. at the War Office, London, on 11th May, 1949.

Ticom
19th May 1949

No. of pages: 4
Copy No. 11

Distribution:-

1. Director.
2. H
3. HR
4. J
5-6 Z 86
7. L
8. L 91
9-16. U.S.L.O.
17. Chief, A.S.A. (E).
18. J.H. Williams, Esq., O.B.E., Signals 6, War Office.

Declassified by D. Janosek,
Deputy Associate Director for Policy and Records
on 12/10/2010 and by L

TOP SECRET

Do NOT Destroy Return to the NSA Technical Library when no longer needed
S-48,711

REPORT ON THE INTERROGATION OF DR. LUZIUS.

Dr. Hans Peter LUZIUS is a mathematician and doctor in natural economy. His last visit to England was in 1933, thereafter he worked in the United States as an employee of the Alliance Insurance Company. He returned to Germany at the beginning of the war, and was called up into the Army in 1941; he was posted almost immediately to OKH, where he worked as a "translator". (It was only in answer to specific questions that he defined his translating activity as the breaking of foreign cyphers). At the end of the war, he became separated from the main OKH organisation, and when it moved south to Reichenhall, he was sent to Flensburg. Since that time, he has lived in Flensburg, Norderhofenden 10, where he may be contacted if required. He speaks almost perfect English, with a strong American accent, and is employed as an interpreter by the British element of C.C.G. He is on holiday with his wife in England, as the guest of a C.C.G. officer, and is returning to Flensburg about 14th May 1949. He stated that he had never previously been questioned on his wartime activities.

2. He had been employed by OKH Inspektorat 7, but professed himself unable to recall the number of the section. He remembered no details of the organisation, nor could he recall the name of a single one of his colleagues! After some pressing, he said that a man named SCHULZ had worked in the English section. At the end of the war, he had lost all contact with other members of the organisation, and had not heard from any of them since; nor did he know where they were at present located.

3. He himself had worked almost entirely on American systems. He was asked to give a description of his work and success on various cyphers. The first system which he remembered was the Strip Cypher, the American name for which was M-94. There were two types, 25-strip and 30-strip, of which OKH had only worked on the former. The 30-strip system was used exculsively on diplomatic and military attaché links, and was worked on by the Foreign Office; although he was not certain of their results, he thought that it had been broken. He described the 25-strip system, and said that in general the same strips were used in a different order each day; on some links, however, the strips were used in the same sequence over a considerable period. The key was indicated by different discriminants, of which he could only remember the first - URSAL.

4. The cypher was solved purely analytically, without any knowledge of the underlying traffic or the type of system; it was only subsequently that they captured some American instructions, which indicated that the system had in fact been in use before the war. Their method of attack was to search for repeats by Hollerith, which they found always occurred on a beat of 25; having identified 20 to 30 passages of cypher text as being in depth, they could then solve each column as a simple substitution, and in this they were considerably assisted by stereotyped openings. They solved most of the traffic on this system, but he thought that the contents were generally relatively unimportant. As instances of its use, he quoted

/meteoroligical

Declassified by D. Janosek,
Deputy Associate Director for Policy and Records
on 12/10/2010 and by [signature]

meteorological traffic in Greenland, and Air Force traffic in the Caribbean.

5. The strip cypher gradually faded out, and was replaced by the M-209 Hagelin at the beginning of the African campaign. This was a better version of the French C-36, which had been solved in the early part of the war; he could give no details as this was before his time. The C-36 had five wheels, whereas the M-209 had six. Here again, solution was purely analytical, and depended upon getting two messages with the same indicators, or a mistake in encypherment. The first break was achieved as the result of a message which was subsequently re-sent with the same indicators but slightly paraphrased, so that the words in the text were slid against each other; their task of diagnosis was also made easier in this case, because, contrary to the instructions which laid down 250 letters as the maximum length of a message, this message was over 700 letters long. They began by guessing a word in the first text, and then trying it out on the second text, utilising the fact that the slide between the two cypher letters would be the same as that between the clear letters. In this way, they could read the text, and work out the cycle and behaviour of the wheels, which enabled them to derive the relative setting. The solution of the absolute setting, which would enable them to read the remaining messages on the day's key, was a more intricate process, and he was unable to recall details, beyond the fact that it was always possible. With practice, they were able to break the relative setting given a minimum of 35 letters of text, although normally they required 60-70 letters. It took them about two hours to derive the absolute setting, after they had broken the initial messages.

6. This was the only method of solution known to them; they could never solve traffic unless they had a depth. The work was done entirely by hand, except that the indicators were sorted by Hollerith. He was unable to say what percentage of keys were read, but thought that it might be about 10%. The only occasion when traffic could be read currently was when they captured some keys in advance in Italy, which continued to be used. There was a theoretical method of solution on one message given at least 1000 letters in a message, but this had never occurred and he did not remember the details.

7. He was then asked whether they had achieved any other successes with this type of machine. He recalled that the Hagelin had been used by the Swedes, in a form known as BC-38. This was similar to the M-209, but with the additional security feature that, whereas with the American machine in the zero position A = Z, B = Y, etc., in the Swedish machine the relationship between these alphabets could be changed. He could not remember whether it had changed daily or for each message. He himself had worked on this machine and had solved a few messages. It had been an unimportant sideline, and he could not remember details; he thought that it had been done by the same method, when two messages occurred with the same indicators. This had only happened very rarely.

8. Asked what he knew about Typex (which he had mentioned during the discussion on Hagelin as having X as a separator), he said immediately "You may rest assured that it was never broken". They had worked on it in the earlier part of the war, and found out the principle, but were never able to solve messages. They had a captured machine without drums; he did not know where it had been obtained. They never captured any drums; even if they had, they would still not have been able to read any traffic. They had given up work on the machine, when they discovered it to be insoluble. All work had been done in the English section, and he could not give any details, nor could he remember who had worked on it. All such work was only done in Berlin.

9. The other main British system of which he had heard was the subtractor recyphering system. Originally, this was solved by searching for repeats by Hollerith; after the African campaign, however, all this traffic changed over to one-time pad, and thereafter no solution could be achieved.

10. Slidex also appeared in 1944, and was solved almost 100%; the system afforded practically no security.

11. The only other American systems which he could recall were the "bigger machine", which was never solved, and of which they never discovered the principle; and various simple codes, of which many were solved. He could not remember any details, other than that one of them had been used in Italy.

12. Military attaché and agents' systems were the responsibility of OKW, and he did not know what degree of success had been achieved.

13. Asked if he knew of any other successes achieved by his organisation, he mentioned the French Hagelin B-211, which was similar to the Russian K-36 or 37. They had captured the Russian machine, but never saw any traffic passed on it. He did not know anything about work on B-211, as it had been before his time. They had also worked on the trans-Atlantic telephone, but he knew no details and said that it had not been solved.

14. There was a section working on the security of the German Enigma, and he had been employed on this for a few days when he first joined the organisation. He had done nothing more than learn the basic principles, and knew nothing of any security appreciations or proposed developments.

15. Asked about OKH cryptanalytic records, he said that these had presumably all gone south with the main body at the end of the war. He did not know what had become of them, but presumed that they had been destroyed - they certainly ought to have been.

16. He knew something of the working of Hollerith machinery from his experience in the Insurance Company, but knew very little of the Hollerith section in OKH, other than the results which they gave him. The section was entirely at the disposal of OKH, and he imagined that the machines were rented. As far as he knew all their

/ machinery

machinery was of the commercial type, except the "D-11", which was used for finding "Parallelstellen" in the strip cypher. OKH did not dispose of any other machinery or cryptanalytic aids.

17. Asked about the work of other German departments, he said that OKH had had contacts with the Foreign Office and OKW; he had had no liaison with them himself, and could give no details. He mentioned the Navy, Air Force and Forschungsamt; about the latter, he did not know any details or whether they had any contacts; he believed that there had been a loose liaison between the Forschungsamt and the Foreign Office. He had also heard talk of a bureau in the S.S., but they certainly had no contacts with this.

18. While LUZIUS appeared quite frank and co-operative, and talked freely when asked specific questions, it seems unlikely that his vagueness and lack of detail on many subjects can be entirely due to the passage of time (the excuse which he made in every case). In particular, it seems improbable that he can still remember all the names of systems, and yet have lost all recollection of his colleagues. When asked if he felt capable of writing up in detail an account of his work, he was very dubious, and said that it would involve starting completely from scratch and would take a very long time. While it is possible that with pressure he might be persuaded to remember more details of his own work and of the general work and organisation of his department, it seems doubtful whether he would be able or prepared to give any detailed information of outstanding value.